Vendor: Palo Alto Networks

Exam Code: NGFW-Engineer

Exam Name: Palo Alto Networks Next-Generation Firewall Engineer

Version: DEMO

QUESTION 1
In a Palo Alto Networks environment, GlobalProtect has been enabled using certificate-based authentication for both users and devices. To ensure proper validation of certificates, one or more certificate profiles are configured.
What function do certificate profiles serve in this context?

A. They store private keys for users and devices, effectively allowing the firewall to issue or reissue certificates if the primary Certificate Authority (CA) becomes unavailable, providing a built-in fallback CA to maintain continuous certificate issuance and authentication.
B. They define trust anchors (root / intermediate Certificate Authorities (CAs)), specify revocation checks (CRL/OCSP), and map certificate attributes (e.g., CN) for user or device authentication.
C. They allow the firewall to bypass certificate validation entirely, focusing only on username / password-based authentication.
D. They provide a one-click mechanism to distribute certificates to all endpoints without relying on external enrollment methods.

Answer: B
Explanation:
In the context of GlobalProtect with certificate-based authentication, certificate profiles are used to ensure proper validation of the certificates. They perform the following functions:
Define trust anchors, which are the root and intermediate Certificate Authorities (CAs) that the firewall trusts to authenticate certificates.
Specify revocation checks, such as CRL (Certificate Revocation List) and OCSP (Online Certificate Status Protocol), to ensure that the certificates being used have not been revoked.
Map certificate attributes, such as the Common Name (CN), which helps in authenticating users and devices based on their certificates.

QUESTION 2
How does a Palo Alto Networks NGFW respond when the preemptive hold time is set to 0 minutes during configuration of route monitoring?

A. It does not accept the configuration.
B. It accepts the configuration but throws a warning message.
C. It removes the static route because 0 is a NULL value
D. It reinstalls the route into the routing information base (RIB) as soon as the path comes up.

Answer: D
Explanation:
When the preemptive hold time is set to 0 minutes in route monitoring, the firewall is configured to immediately reinstall the route into the Routing Information Base (RIB) as soon as the monitored path comes up. This essentially means that the firewall will not wait for any predefined hold time before reestablishing the route once the monitoring condition is met, ensuring a faster recovery of the route.

QUESTION 3
After an engineer configures an IPSec tunnel with a Cisco ASA, the Palo Alto Networks firewall generates system messages reporting the tunnel is failing to establish. Which of the following actions will resolve this issue?

A. Ensure that an active static or dynamic route exists for the VPN peer with next hop as the tunnel interface.
B. Configure the Proxy IDs to match the Cisco ASA configuration.

C. Check that IPSec is enabled in the management profile on the external interface.
D. Validate the tunnel interface VLAN against the peer's configuration.

Answer: B
Explanation:
The Proxy IDs (or Traffic Selectors) define the local and remote subnets that are allowed to communicate over the IPSec tunnel. If the Proxy IDs on the Palo Alto Networks firewall do not match the configuration on the Cisco ASA, the tunnel will fail to establish because the firewalls won't agree on which traffic to encrypt. Ensuring that the Proxy IDs match between the Palo Alto Networks firewall and the Cisco ASA will resolve the issue.

QUESTION 4
Which configuration in the LACP tab will enable pre-negotiation for an Aggregate Ethernet (AE) interface on a Palo Alto Networks high availability (HA) active/passive pair?

A. Set Transmission Rate to "fast."
B. Set passive link state to "Auto."
C. Set "Enable in HA Passive State."
D. Set LACP mode to "Active."

Answer: C
Explanation:
In a High Availability (HA) active/passive pair configuration, when setting up an Aggregate Ethernet (AE) interface, enabling the "Enable in HA Passive State" option allows the interface to participate in LACP (Link Aggregation Control Protocol) even when the system is in the passive state. This ensures that the pre-negotiation of the LACP link occurs, allowing the link aggregation to be ready as soon as the firewall becomes active.

QUESTION 5
When integrating Kubernetes with Palo Alto Networks NGFWs, what is used to secure traffic between microservices?

A. Service graph
B. Ansible automation modules
C. Panorama role-based access control
D. CN-Series firewalls

Answer: D
Explanation:
When integrating Kubernetes with Palo Alto Networks NGFWs, the CN-Series firewalls are specifically designed to secure traffic between microservices in containerized environments. These firewalls provide advanced security features like Application Identification (App-ID), URL filtering, and Threat Prevention to secure communication between containers and microservices within a Kubernetes environment.

QUESTION 6
When configuring a Zone Protection profile, in which section (protection type) would an NGFW engineer configure options to protect against activities such as spoofed IP addresses and split handshake session establishment attempts?

A. Flood Protection

B. Protocol Protection
C. Packet-Based Attack Protection
D. Reconnaissance Protection

Answer: B
Explanation:
In the context of a Zone Protection profile, Protocol Protection is the section used to configure protections against activities such as spoofed IP addresses and split handshake session establishment attempts. These types of attacks typically involve manipulating protocol behaviors, such as IP address spoofing or session hijacking, and are mitigated by the Protocol Protection settings.

QUESTION 7
For which two purposes is an IP address configured on a tunnel interface? (Choose two.)

A. Use of dynamic routing protocols
B. Tunnel monitoring
C. Use of peer IP
D. Redistribution of User-ID

Answer: AB
Explanation:
Use of dynamic routing protocols: An IP address is needed on the tunnel interface to participate in dynamic routing protocols (like OSPF, BGP, etc.) over the tunnel. This allows the firewall to advertise routes and receive updates over the tunnel.
Tunnel monitoring: The IP address on the tunnel interface can also be used for monitoring the tunnel's status. Tunnel monitoring (such as IPSec tunnel monitoring) requires an IP address on the tunnel interface to check the health and availability of the tunnel.

QUESTION 8
Which PAN-OS method of mapping users to IP addresses is the most reliable?

A. Port mapping
B. GlobalProtect
C. Syslog
D. Server monitoring

Answer: D
Explanation:
Server monitoring is the most reliable method for mapping users to IP addresses in PAN-OS. This method allows the firewall to monitor specific servers, such as Microsoft Active Directory (AD) or LDAP servers, to dynamically retrieve and update user-to-IP mappings. It provides a more accurate and up-to-date mapping of users to their associated IP addresses, as it directly queries user databases in real time.

QUESTION 9
In an active/active high availability (HA) configuration with two PA-Series firewalls, how do the firewalls use the HA3 interface?

A. To forward packets to the HA peer during session setup and asymmetric traffic flow
B. To exchange hellos, heartbeats, HA state information, and management plane synchronization

for routing and User-ID information

C. To synchronize sessions, forwarding tables, IPSec security associations, and ARP tables between firewalls in an HA pair
D. To perform session cache synchronization among all HA peers having the same cluster ID

Answer: D
Explanation:
In an active/active HA configuration with two PA-Series firewalls, the HA3 interface is used primarily for the exchange of HA state information between the firewalls. This includes:
Hellos and heartbeats to monitor the status of the HA peer. Synchronization of management plane data, which includes critical routing and User-ID information.

QUESTION 10
A PA-Series firewall with all licensable features is being installed. The customer's Security policy requires that users do not directly access websites. Instead, a security device must create the connection, and there must be authentication back to the Active Directory servers for all sessions. Which action meets the requirements in this scenario?

A. Deploy the transparent proxy with Web Cache Communications Protocol (WCCP).
B. Deploy the Next-Generation Firewalls as normal and install the User-ID agent.
C. Deploy the Advanced URL Filtering license and captive portal.
D. Deploy the explicit proxy with Kerberos authentication scheme.

Answer: D
Explanation:
In this scenario, the customer requires that users do not directly access websites and that a security device (the firewall) manages the connection, while also ensuring that there is authentication back to the Active Directory (AD) servers for all sessions. The explicit proxy with Kerberos authentication is the best solution because:
The explicit proxy allows the firewall to intercept user web traffic and manage the connections on behalf of users.
Kerberos authentication ensures that the user's identity is validated against the Active Directory servers before the session is allowed, fulfilling the authentication requirement.

QUESTION 11
What must be configured before a firewall administrator can define policy rules based on users and groups?

A. User Mapping profile
B. Authentication profile
C. Group mapping settings
D. LDAP Server profile

Answer: C
Explanation:
Before a firewall administrator can define policy rules based on users and groups, the Group Mapping settings must be configured. These settings enable the firewall to map users to their respective Active Directory (AD) groups. This mapping allows the firewall to use user and group information to create policy rules based on group membership.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: ASTR14